ROUTING AND TRANSMITTAL SLIP

11 Mar 88

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. C/PRS		
2.		
3.		
4.		
5.		

X	Action		File		Note and Return
	Approval		For Clearance		Per Conversation
	As Requested		For Correction		Prepare Reply
	Circulate		For Your Information		See Me
	Comment		Investigate		Signature
	Coordination		Justify		

REMARKS

EO requests this be reviewed and compared against our previous input. I was not sure if you or Jeanne worked this.

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
STAT	Phone No.

5041-102 OPTIONAL FORM 41 (Rev. 7-76)

Declassified in Part - Sanitized Copy Approved for Release
2013/03/04 : CIA-RDP91B00390R000300320007-5

[redacted]

ROUTING AND TRANSMITTAL SLIP

Date: 8 Feb 88

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. DD/PTS COORD		
2. C/CSD Signature		
3. AD/CO		
4. OC-CSD/Maryann for distribution		
5.		

OS REGISTRY
FEB 1988

	Action		File		Note and Return
	Approval		For Clearance		Per Conversation
	As Requested		For Correction		Prepare Reply
	Circulate		For Your Information		See Me
	Comment		Investigate		Signature
	Coordination		Justify		

REMARKS

Registry Copy

NTISSC file

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
STAT OC-CSD/TLO	Phone No.

5041-102 ☆ U.S. GPO: 1986—491-247/40012 OPTIONAL FORM 41 (Rev. 7-76) Prescribed by GSA FPMR (41 CFR) 101-11.206

[redacted]

CONFIDENTIAL

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Draft National Policy for Granting Access to U.S. Classified Cryptographic Information

25X1

FROM: C/OC-CSD

25X1

EXTENSION

NO. OC-4541-88

DATE

25X1

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. OIT				
2.				
3. DDA 7D18 Hqs				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

25X1

FORM 610 USE PREVIOUS

CONFIDENTIAL

OC-4541-88
10 FEB 1988

MEMORANDUM FOR: Deputy Director for Administration

25X1 FROM: [redacted]
Chief, Communications Security Division, OC

SUBJECT: Draft National Policy for Granting Access to U.S.
25X1 Classified Cryptographic Information [redacted]

REFERENCES: A. NTISSC-008/88, dtd 25 Jan 88, Same Subject

B. NTISSC-080/87, dtd 10 Jul 87, Same Subject

C. OC-4811-87, dtd 17 Aug 87, Same Subject

1. The attachment to this memorandum provides the background leading up to Reference A. Also provided is a discussion of the political ramifications plus recommendations for the CIA representative to NTISSC for use at the 17 February 1988
25X1 meeting. [redacted]

2. This memorandum has been coordinated with the Office of
25X1 Security. [redacted]
25X1

[redacted]

Attachment

25X1 [redacted]

CONFIDENTIAL

SUBJECT: Draft National Policy for Granting Access to U.S.
25X1 Classified Cryptographic Information [redacted]

CONCUR:

25X1 [redacted]

for Director of Security

8 FEB 1988
Date

Attachment To: OC-4541-88

SUBJECT: Draft National Policy for Granting Access to U.S. Classified Cryptographic Information 25X1

I. BACKGROUND

A. Reference C was the Office of Communications' response to Reference B. Reference B draft policy required that all personnel being granted a U.S. Government cryptographic clearance undergo a "polygraph examination to be randomly administered not less than once every five years." Reference C was an attempt to tighten up the draft language to require a polygraph prior to granting a cryptographic clearance and urged that an interagency agreement on certification be attained. Reference C further suggested a subset of the 4C program be used to verify clearances once interagency certification was agreed upon. Subsequently, the Central Intelligence Agency (CIA) representative to NTISSC concurred with Reference B language, as written. 25X1

B. Reference A, on which NTISSC members must be prepared to vote at the 17 February 1988 meeting, is a weaker version of Reference B as it pertains to counterintelligence polygraph examinations. Reference A states that each agency or department head shall "ensure that a capability exists within the department or agency to obtain the resources necessary to administer any polygraph examinations." This language effectively negates requiring a polygraph examination either before or after a cryptographic clearance is granted. Reference A language is further diluted from that of Reference B by removing the caveat that unofficial travel in certain foreign countries will be approved prior to travel. 25X1

C. Both References A and B language requires that Federal departments and agencies shall "accept, as valid, cryptographic access certificates granted by other Federal departments and agencies." 25X1

25X1

SUBJECT: Draft National Policy for Granting Access to U.S.
25X1 Classified Cryptographic Information

II. DISCUSSION

A. It is our understanding that counterintelligence polygraphs is an extremely political subject in the telecommunications community and in congress. There are varying degrees of support and opposition. The opposition group is more vociferous than the support group and could possibly object to Reference A even though the language does not require a polygraph, but simply mentions it.

B. We have been advised there was a general feeling among the polygraph supporters at the last NTISSC meeting that just getting the subject of polygraphs into the the language was a step in the right direction. The supporters felt that a community agreement could not be reached if the language reflected that a polygraph was required. It was also felt that it was important to get community agreement to require a special clearance for cryptographic access where no community requirement in this area now exists.

III. CONCLUSION

A. If Reference A language is retained and polygraph examinations are not required for granting of a cryptographic clearance, the CIA cannot "accept, as valid" other agency certificates. Doing so would abrogate our own stringent controls and leave us vulnerable to the human element, i.e. Walker/Whitworth.

B. We feel that a community wide agreement for cryptographic clearances is very important, but for the reasons stated in paragraph A, above, it is recommended the CIA representative to NTISSC lobby to retain the language of Reference B requiring polygraph examinations.

C. As an alternative, removal of the Reference A, Section V, paragraph e, would allow us to support the remainder of the document in the interest of fostering a community wide cryptographic clearance.

D. If Reference A is voted on without change, we recommend a dissenting vote be cast.

NTISSC
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

OFFICE OF THE EXECUTIVE SECRETARY

NTISSC-008/88
25 January 1988

MEMORANDUM FOR THE MEMBERS AND OBSERVERS, NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

SUBJECT: 17 February 1988 Meeting of the NTISSC - **INFORMATION MEMORANDUM**

1. This memorandum forwards the agenda for the 17 February meeting of the NTISSC (Enclosure 1). The meeting will be held from 1000 to 1200 hours, in Room C2E91, Operations Building #3, of the National Security Agency, located on Erskine Road, Ft. George G. Meade, Maryland.

2. Access to Operations Building #3 will be via Gatehouse #8 located on Erskine Road. Attendees are requested to report to the Visitors Control Center where they will be met and escorted to the conference room. As entry into this facility is controlled, it is imperative that names of attendees be reflected on the access list. Please notify the NTISSC Secretariat **by 11 February 1988**, if you plan to attend this meeting (Phone: 301-688-7355/688-7736). For your convenience, Enclosure 3 is a map of the NSA facility which includes travel and parking information.

3. Members and observers are reminded that advance written notification to the Chairman is required, if an alternate representative will be in attendance. This written notification must identify the alternate and specifically state the named individual is empowered to speak on behalf of the represented agency.

4. Agenda Item IV, "Proposed National Policy for Granting Access to U.S. Classified Cryptographic Information," was reviewed by the Committee in the July/August 1987 timeframe (forwarded via NTISSC-080/87, dated 10 July 1987). As a result of concerns raised during the review process, this policy proposal has been modified and a copy is provided at Enclosure 2 (changes are annotated by an asterisk (*) in the right-hand margin). Members are requested to be prepared to vote on this policy proposal at the 17 February meeting.

STAT

Executive Secretary

3 Enclosures

AGENDA

TWELFTH MEETING

OF THE

NATIONAL TELECOMMUNICATIONS AND

INFORMATION SYSTEMS SECURITY COMMITTEE

I. Approval of the 16 November 1987 NTISSC Meeting Minutes

.... Acting Chairman, NTISSC
Dr. Thomas P. Quinn

II. Status of Committee Actions

.... Executive Secretary, NTISSC

STAT [redacted]

III. Subcommittee Reports

.... Chairman, STS
Mr. William A. Bayse

.... Chairman, SAISS

STAT [redacted]

IV. Proposed "National Policy for Granting Access to U.S. Classified Cryptographic Information" - **FOR VOTE**

.... Acting Chairman, NTISSC
Dr. Thomas P. Quinn

V. Proposed "National Policy on Control of Compromising Emanations" & Proposed NTISSI, "Tempest Countermeasures for Facilities"

.... Chairman, STS
Mr. William A. Bayse

ENCLOSURE 1

DRAFT

FOREWORD

Pursuant to the authority of Executive Order 12333 and National Security Decision Directive 145, and in accordance with Executive Order 12356, Section 4.2, there is hereby established a program governing access to U.S. classified cryptographic information. It is recognized that the technically sophisticated cryptographic systems employed by the United States Government can be compromised if the human element is not subject to certain reasonable controls regarding access to the U.S. classified cryptographic information supporting these systems. Therefore, NTISSP No. XXXX was developed by the National Telecommunications and Information Systems Security Committee (NTISSC) for the purpose of reinstating formal cryptographic access as a means of preventing loss or unauthorized disclosure of U.S. classified cryptographic information.

Within the scope of this policy, reference is made to the use of the non-lifestyle, counterintelligence scope polygraph examination. It should be noted that the polygraph need not be used as a prescreening mechanism for determining cryptographic access. Rather, it is intended that each department and agency utilize the potential deterrent factor of the polygraph as it deems necessary and at its own discretion. *

ENCLOSURE 2

DRAFT

DRAFT

NATIONAL POLICY FOR GRANTING ACCESS TO U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION

SECTION I - POLICY

1. Certain U.S. classified cryptographic information, the loss of which could cause serious or exceptionally grave damage to U.S. national security, requires special access controls. Accordingly, this policy establishes a formal cryptographic access program whereby access to certain U.S. classified cryptographic information shall only be granted to individuals who satisfy the criteria set forth herein.

SECTION II - DEFINITION

2. As used in this policy, U.S. classified cryptographic information is defined as:

a. TOP SECRET and SECRET, CRYPTO designated, key and authenticators.

b. All cryptographic media which embody, describe, or implement classified cryptographic logic; this includes full maintenance manuals, cryptographic descriptions, drawings of cryptographic logics, specifications describing a cryptographic logic, cryptographic computer software, or any other media which may be specifically identified by the National Manager.

SECTION III - CRITERIA

3. An individual may be granted access to U.S. classified cryptographic information, only if that individual:

a. Is a U.S. citizen;

b. Is an employee of the U.S. Government, is a U.S. Government contractor or employee of such contractor, or is employed as a U.S. Government representative (including consultants of the U.S. Government);

c. Requires access to perform official duties for, or on behalf of, the U.S. Government;

d. Possesses a security clearance appropriate to the classification of the U.S. cryptographic information to be accessed;

e. Possesses a valid need-to-know for the information; *

DRAFT

f. Receives a security briefing appropriate to the U.S. classified cryptographic information to be accessed;

g. Acknowledges the granting of access by signing a Cryptographic Access Certificate; and

h. Voluntarily consents to be subject to a non-lifestyle, counterintelligence scope polygraph examination which shall be administered in accordance with department or agency directives and applicable law. The examining official shall only select questions which concern espionage, sabotage, or questions which relate to the unauthorized disclosure of U.S. classified cryptographic information.

4. All persons indoctrinated for cryptographic access within the guidelines of this program must comply with requirements, prescribed in department or agency security directives, regarding unofficial foreign travel or contacts with foreign nationals.

SECTION IV - APPLICATION

5. This policy shall apply to all individuals who are required to have access to U.S. classified cryptographic information in the performance of their normal duties. Accordingly, the provisions of this policy apply to those individuals assigned:

a. As COMSEC custodians or alternates.

b. As producers or developers of cryptographic key or logic.

c. As cryptographic maintenance or installation technicians.

d. To facilities where cryptographic keying materials are generated or stored.

e. To prepare, authenticate, or decode valid or exercise nuclear control orders.

f. In secure telecommunications facilities located in fixed ground facilities or on board ships.

g. Any other responsibility with access to U.S. classified cryptographic information which is specifically identified by the head of a department or agency.

SECTION V - RESPONSIBILITIES

6. The heads of Federal departments and agencies shall:

a. Implement the provisions of this policy within their respective department or agency. *

b. Ensure that a capability exists within the department or agency to obtain the resources necessary to administer any polygraph examinations. This may be accomplished either by directly programming and funding for these resources or by executing agreements or arrangements to utilize the existing resources of another department or agency. *

c. Develop and administer a "Cryptographic Access Briefing" which shall address the specific security concerns of the department or agency; an example of such a briefing is presented in Annex A. *

d. Prepare a "Cryptographic Access Certificate" which shall be signed by all individuals granted cryptographic access in accordance with this program; an example of such a certificate is presented in Annex B. The Cryptographic Access Certificate shall be made a permanent part of the individual's official security records and shall be accounted for in accordance with department or agency directives concerning retention of security clearance/access certificates. *

e. Accept, as valid, Cryptographic Access Certificates granted by other Federal departments and agencies. * deleted

f. Ensure that applicable department or agency security directives contain requirements for reporting unofficial foreign travel and contacts with foreign nationals. *

SECTION VI - EXCEPTIONS

7. Exceptions to this policy may be approved by department or agency heads to meet exigent operational needs. Records of exceptions granted shall be made available to the National Manager on request. *

2 Encls:

1. Annex A, Cryptographic Access Briefing (SAMPLE)
2. Annex B, Cryptographic Access Certificate (SAMPLE)

SAMPLE

CRYPTOGRAPHIC ACCESS BRIEFING

You have been selected to perform duties that will require access to U.S. classified cryptographic information. It is essential that you be made aware of certain facts relevant to the protection of this information before access is granted. You must know the reason why special safeguards are required to protect U.S. classified cryptographic information. You must understand the directives which require these safeguards and the penalties you will incur for willful disclosure of this information to unauthorized persons.

U.S. classified cryptographic information is especially sensitive because it is used to protect classified information which relates to our national security. Disclosure of this information to unauthorized persons, could result in irreparable damage to the United States. Any particular piece of cryptographic keying material and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of a cryptographic system is breached at any point, all information protected by the system may be compromised. The safeguards placed on U.S. classified cryptographic information are a necessary component of government programs to ensure that our Nation's vital secrets are not compromised.

Because access to U.S. classified cryptographic information is granted on a strict need-to-know basis, you will be given access to only that cryptographic information necessary in the performance of your duties. You are required to become familiar with (insert, as appropriate, department or agency implementing directives covering the protection of cryptographic information). Cited directives are attached in a briefing book for your review at this time.

Especially important to the protection of U.S. classified cryptographic information is the timely reporting of any known or suspected compromise of this information. If a cryptographic system is compromised, but the compromise is not reported, the continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps can be taken to lessen an adversary's advantage gained through the compromise of the information.

As a condition of access to U.S. classified cryptographic information, you must voluntarily consent to be subject to a non-lifestyle, counterintelligence scope polygraph examination. This examination will be administered in accordance with the provisions of (insert appropriate department or agency directive) and applicable law. This polygraph examination will only encompass questions concerning espionage, sabotage, or

questions relating to unauthorized disclosure of classified information.

You have the right to refuse to be subject to the non-lifestyle, counterintelligence scope polygraph examination. Such refusal will not be cause for adverse action but may result in your being denied access to U.S. classified cryptographic information. If you do not, at this time, wish to sign such a consent as a part of executing the Cryptographic Access Certificate, this briefing will be terminated at this point and the briefing administrator will so notate the Cryptographic Access Certificate.

* * * * * * * * * * * * * * * * * * *

You should know that intelligence services of some foreign governments prize the acquisition of U.S. classified cryptographic information. They will go to extreme lengths to compromise U.S. citizens and force them to divulge cryptographic techniques and materials that protect the nation's secrets around the world. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion to divulge U.S. classified cryptographic information. You should be alert to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, U.S. classified cryptographic information and thus avoid highlighting yourself to those who would seek the information you possess. Any attempt, either through friendship or coercion, to gain knowledge regarding the U.S. classified cryptographic information you have must be reported immediately to (insert appropriate security office).

In view of the risks noted above, unofficial travel to certain communist or other designated countries may require the prior approval of (insert appropriate security office). It is essential that you contact (insert appropriate security office) if such unofficial travel becomes necessary.

Finally, you must know that, should you willfully disclose to any unauthorized persons any of the U.S. classified cryptographic information to which you will have access, you may be subject to administrative and personnel security actions as well as prosecution under the Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States.

DRAFT

CRYPTOGRAPHIC ACCESS CERTIFICATE

INSTRUCTION

Section I of this certificate must be executed before an individual may be granted access to U.S. classified cryptographic information. Section II will be executed when the individual no longer requires such access. This certificate (original) will be made a permanent part of the official security records of the individual concerned.

SECTION I

AUTHORIZATION FOR ACCESS TO U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION

a. I understand that I am being granted access to U.S. classified cryptographic information. I understand that my being granted access to this information involves me in a position of special trust and confidence concerning matters of national security. I hereby acknowledge that I have been briefed concerning my obligations with respect to such access.

b. I understand that safeguarding U.S. classified cryptographic information is of the utmost importance and that the loss or compromise of such information could lead to irreparable damage to the United States. I understand that I am obligated to protect U.S. classified cryptographic information and I have been instructed in the special nature of this information and the reasons for the protection of such information. I agree to comply with any special instructions, issued by my security office, regarding unofficial foreign travel or contacts with foreign nationals. I voluntarily consent to be subject to a non-lifestyle, counterintelligence scope polygraph examination to be administered in accordance with (insert appropriate department or agency directive) and applicable law.

c. I understand fully the information presented during the briefing I have received. I have read this certificate and my questions, if any, have been satisfactorily answered. I acknowledge that the briefing officer has made available to me the provisions of Title 18, United States Code, Sections 641, 793, 794, 798, and 952. I understand that, if I willfully disclose to any unauthorized person any of the U.S. classified cryptographic information to which I might have access, I may be subject to prosecution under the UCMJ and/or the criminal laws of the United States. I understand and accept that unless

DRAFT

I am released in writing by an authorized representative of (insert appropriate security office) the terms of this certificate and my obligation to protect all U.S. classified cryptographic information to which I may have access, apply during the time of my access and at all times thereafter.

ACCESS GRANTED THIS DAY OF 19

SIGNATURE NAME/GRADE,RANK,RATING/SSN

SIGNATURE OF ADMINISTERING OFFICIAL NAME/GRADE/OFFICIAL POSITION

SECTION II

TERMINATION OF ACCESS TO U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION

I am aware that my authorization for access to U.S. classified cryptographic information is being withdrawn. I fully appreciate and understand that the preservation of the security of this information is of vital importance to the welfare and defense of the United States. I certify that I will never divulge any U.S. classified cryptographic information I acquired, nor discuss with any person any of the U.S. classified cryptographic information to which I have had access, unless and until freed from this obligation by unmistakable notice from proper authority. I have read this agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Title 18, United States Code, Sections 641, 793, 794, 798, and 952; and Title 50, United States Code, Section 783(b).

ACCESS WITHDRAWN THIS DAY OF 19

SIGNATURE NAME/GRADE, RANK, RATING/SSN

SIGNATURE OF ADMINISTERING OFFICIAL NAME/GRADE/OFFICIAL POSITION

DRAFT

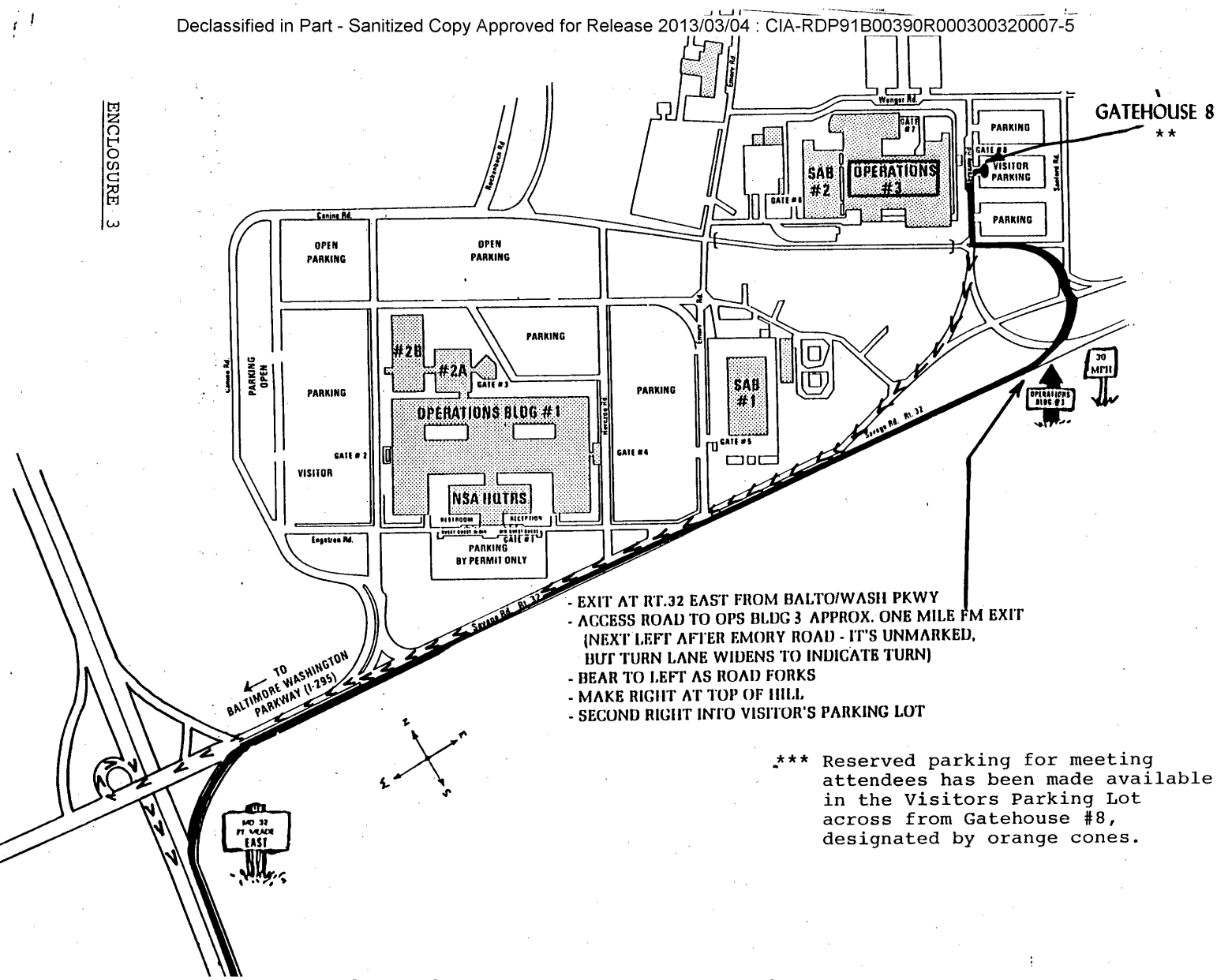
DRAFT

PRIVACY ACT STATEMENT

Authority to request Social Security Number (SSN) is Executive Order 9397. Routine and sole use of the SSN is to identify the individual precisely when necessary to certify access to U.S. classified cryptographic information. While disclosure of your SSN is voluntary, failure to do so may delay certification and in some cases, prevent original access to U.S. classified cryptographic information.

SIGNATURE DATE

ENCLOSURE 3



- EXIT AT RT.32 EAST FROM BALTO/WASH PKWY
- ACCESS ROAD TO OPS BLDG 3 APPROX. ONE MILE FM EXIT (NEXT LEFT AFTER EMORY ROAD - IT'S UNMARKED, BUT TURN LANE WIDENS TO INDICATE TURN)
- BEAR TO LEFT AS ROAD FORKS
- MAKE RIGHT AT TOP OF HILL
- SECOND RIGHT INTO VISITOR'S PARKING LOT

*** Reserved parking for meeting attendees has been made available in the Visitors Parking Lot across from Gatehouse #8, designated by orange cones.

25 January 1988

NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

Acting Chairman	Dr. Thomas P. Quinn Acting Assistant Secretary of Defense (Command, Control, Communications and Intelligence) The Pentagon, Room 3E172 Washington, D.C. 20301	695-0348
STAT Executive Secretary	[redacted] Executive Secretary, NTISSC National Security Agency Operations Building #3, Room COW89 Fort George G. Meade, Md. 20755-6000	688-7355
NSC	Office of Special Assistant to the President for National Security Affairs National Security Council Staff Old Executive Office Building, Room 300 Washington, D.C. 20506	395-3334
State	Mr. Robert L. Caffrey Deputy Assistant Secretary for Communications Department of State, Room 44A26 2201 C. Street, N.W. Washington, D.C. 20520	647-1000
Treasury	Mr. Roger M. Cooper Deputy Assistant Secretary for Information Systems Department of the Treasury,Room 2415 15th and Pennsylvania Avenue, N.W. Washington, D.C. 20220	566-5847
Defense	Ms. Diane Fountaine Director, Information Systems, ASDC3I The Pentagon, Room 3E187 Washington, D.C. 20301-3040	697-7181
Attorney General	Mr. D. Jerry Rubino Director, Security Staff Justice Management Division Main Justice Building, Room 6525 Washington, D.C. 20530	633-2094

OMB	Mr. Arnold E. Donahue Chief, Intelligence Branch National Security Division Office of Management and Budget, Room 8215 17th and Pennsylvania Avenue Washington, D.C. 20503	395-4800
STAT		
DCI	Mr. William F. Donnelly Deputy Director for Administration 2DOO HQS Central Intelligence Agency Washington, D.C. 20505	
Commerce	Mr. Charles G. Schott Deputy Assistant Secretary for Communications and Information H.C. Hoover Building, Room 4898 14th and Constitution Avenue,N.W. Washington, D.C. 20230	377-1830
Transportation	(Unclassified) Mr. Sanford L. Glassman Chief, Telecommunications Division (M-33) Office of the Secretary, Room 9112 Department of Transportation 400 7th Street, S.W. Washington, D.C. 20590	426-2022
	(Classified) Department of Transportation Classified Control Point Nassif Building, Room 10325 ATTN: S. L. Glassman 400 7th Street, S.W. Washington, D.C. 20590	
Energy	Mr. John W. Polk Director, Office of Computer Services and Telecommunications Management Department of Energy Room CA-311, MA-25 (GTN) Washington, D.C. 20545	353-3685
JCS	VADM Jerry O. Tuttle, USN Director, C3S OJCS The Pentagon, Room 2D860 Washington, D.C. 20301	695-6478

GSA	Mr. George F. Flynn, Jr. NSEP Division Room G-13 (KJN) General Services Administration 18th and F Streets SW Washington, D.C. 20405	566-0843
FBI	Mr. William A. Bayse Assistant Director, Technical Services Division Federal Bureau of Investigation Room 7159 10th and Pennsylvania Avenue, N.W. Washington, D.C. 20535	324-5350
FEMA	(Unclassified) Mr. Bruce J. Campbell Assistant Associate Director for Information Resources Management Federal Emergency Management Agency 500 C. Street, S.W., Room 521 Washington, D.C. 20472 (Classified) Federal Emergency Management Agency ATTN: Classified Document Control Office, Room M-01 500 C Street, S.W. Washington, D.C. 20472	646-2965
Army	MG Robert P. Morgan, USA Vice Director of Information Systems for C4 HQ DA (SAIS-ZB) The Pentagon, Room 3E458 Washington, D.C. 20310-0700	695-6604
Navy	RADM Roger L. Rich, Jr., USN Director, Naval Communications Division (OP-941) Office of the Chief of Naval Operations Department of the Navy The Pentagon, Room 5A718 Washington, D.C. 20305-2000	695-7284
Air Force	Brig Gen Robert H. Ludwig Assistant Chief of Staff, Systems for Command, Control, Communications and Computers HQ USAF/SC The Pentagon, Room 5B477 Washington, D.C. 20330-5190 and,	695-4440

	Brig Gen Denis M. Brown, USAF Deputy Assistant Chief of Staff Systems for Command, Control Communications and Computers HQ USAF/SC The Pentagon, Room 5B477 Washington, D.C. 20330-5190	695-6324
Marine Corps	Dr. James Painter Deputy Director, C4 HQ Marine Corps (Code CC) U.S. Marine Corps Annex, Room 3016 Washington, D.C. 20380-0001	694-2628
STAT DIA	[redacted] Deputy Director, for DODIIS Engineering DIAC RSE Defense Intelligence Agency Washington, D.C. 20340-3081	373-2967
STAT NSA	[redacted] Deputy Director for Information Security National Security Agency Fort George G. Meade, Maryland 20755-6000	688-8111
NCS	Lt Gen John T. Myers, USA Manager, National Communications System Washington, D.C. 20305-2010	692-0018

As Observers:

FCC	Mr. Edward J. Minkel Managing Director, Federal Communications Commission Room 411, ATTN: Internal Review & Security Div. 1919 M. Street, N.W. Washington, D.C. 20554 (Classified) ATTN: Security Officer, Room 411 Federal Communications Commission 1919 M. Street, N.W. Washington, D.C. 20554	632-6390
DCA	Mr. E. William Harding Acting Director, Defense Communications System Organization Room 3140 Washington, D.C. 20305	692-9048

NASA	(TS and below) Mr. Robert O. Aller Associate Administrator for Space Tracking and Data Systems Code T, NASA Headquarters, Room 500 600 Independence Avenue Washington, D.C. 20546	453-2019
	(Above TS) Mr. Robert O. Aller NASA Headquarters Code LD, Room 7112 400 Maryland Avenue Washington, D.C. 20546	
STAT Chairman SAISS	[redacted] Director, National Computer Security Center Airport Square #11 National Security Agency Fort George G. Meade, Maryland 20755-6000	859-4371
NRC	(Unclassified) Mr. Raymond J. Brady Director, Division of Security U.S. Nuclear Regulatory Commission 7735 Old Georgetown Road Bethesda, MD. 20814	492-4100
	(Classified) U.S. Nuclear Regulatory Commission ATTN: SSO/Mr. Brian Reppert 7915 Eastern Avenue, Room 261 Willste Building Silver Spring, MD. 20910	
ICS	Mr. William F. Lackman, Jr. Deputy Director, Intelligence Community Staff Community Headquarters Building Washington, D.C. 20505	376-5612

CONFIDENTIAL

SUBJECT: Draft National Policy for Granting Access to U.S.
25X1 Classified Cryptographic Information [redacted]

CONCUR:

_____ _____
Director of Security Date

25X1 Orig: OC-CSD [redacted] (2 Feb 88)
25X1 2nd page retyped: O-ES/OS: [redacted] (9 Feb 88)

Distribution:
Orig - Addressee w/att
1 - D/OS w/att
1 - OC-CSD Chrono w/o att
1 - OC-CSD Subject File w/att
1 - OC-OL-ISC w/o att